

PASSWORD EXPOSURE ELIMINATION FOR DIGITAL SIGNATURE
COUPLING WITH A HOST IDENTITY

ABSTRACT

A method for creating a proof of possession confirmation for inclusion by a certification authority into a digital certificate, the digital certificate for use by an end user, is disclosed. In an exemplary embodiment of the invention, the method includes receiving from the certification authority, in response to a certificate request by the end user, a plurality of data fields corresponding to a target host system, the end user, and a form of proof of identity possession by the end user. The content of the plurality of data fields is analyzed and the accuracy thereof is verified. If the plurality of data fields is verified as accurate, then a signed object is sent to the certification authority, the signed object comprising the proof of possession confirmation.

09637050